Interim e-Authentication Gateway
CONCEPT OF OPERATIONS

February 2003

Prepared by:

3150 Fairview Park Drive
Falls Church, VA 22042

TABLE OF CONTENTS

LIST OF FIGURES **PAGE**

1.0 Introduction

As part of President Bush's Management Agenda, the President's Management Council in November 2001 identified and approved 24 e-Government (e-Gov) initiatives across four segments - citizen, business, government, and internal operations - to make government more responsive to citizens and to help it operate more efficiently. As many of the services and transactions offered by the initiatives involve the transmission of sensitive or private information, trust is crucial for e-Government to be successful. The key to that trust is the development of authentication solutions that ensure the right parties have the right access to the right information.

To streamline the delivery of authentication services to those initiatives, the e-Authentication Initiative was launched and tasked with providing a common authentication service and infrastructure. This is referred to as the Interim e-Authentication Gateway.

1.1 Background

Following the launch of the e-Authentication Initiative, representatives from all of the e-Gov initiatives began to identify and define Interim e-Authentication Gateway technical and policy concepts and requirements, based on the following mission, goals, and objectives:

- **Mission:** Public Trust in the security of information exchanged over the Internet plays a vital role in the e-Gov transformation. The e-Authentication Initiative makes this trust possible.

- **Goals:**
  - To build and enable mutual trust needed to support wide-spread use of electronic interactions between the public and government, and across governments.
  - To minimize the burden on the public when obtaining trusted electronic services from the government, and across the governments.
  - Deliver common interoperable authentication solutions, ensuring they are an appropriate match for the levels of risk and business needs of each e-Government (e-Gov) initiative.

- **Objectives:**
  - Define operational concepts, to include critical success factors and requirements, in conjunction with each e-Gov initiative.
  - Define authentication requirements analyses - completed December 2002.
  - Develop an initial authentication capability that will support multiple levels of assurance.
  - Develop a functional Interim Gateway - completed September 2002.
  - Develop a FirstGov Interface with the Interim Gateway.

- Have two e-Gov applications using the Interim Gateway for authentication services - completed September 2002.
- Have a Production Gateway by September 2003.

Figure 1.1-1, e-Gov Initiatives, illustrates the relationship of the e-Authentication initiative as a cross-cutting project, that provides and supports authentication services for all of the initiatives.

Figure 1.1-1. e-Gov Initiatives

Figure 1.1-2, Interim e-Authentication Gateway Requirements Development Process, illustrates the flow and process of gathering information and inputs from industry and government for the purposes of developing an Interim e-Authentication Gateway Requirements definition.

The Interim e-Authentication Gateway Development Team developed an initial set of high-level concepts that described preliminary functional requirements and policy definitions. These concepts were discussed in open meetings with commercial vendors in the market place. Those discussions provided an opportunity for the government to interface with industry in an effort determine if the initial functional requirements were feasible and commercially available today.

In addition, two open forums were conducted with industry and government agencies to provide more opportunity for feedback on the Interim e-Authentication Gateway

concepts. Following those meetings, a "directed" Request for Information (RFI) was released as an effort to acquire specific input from industry regarding detailed technical, policy, and contract related issues.

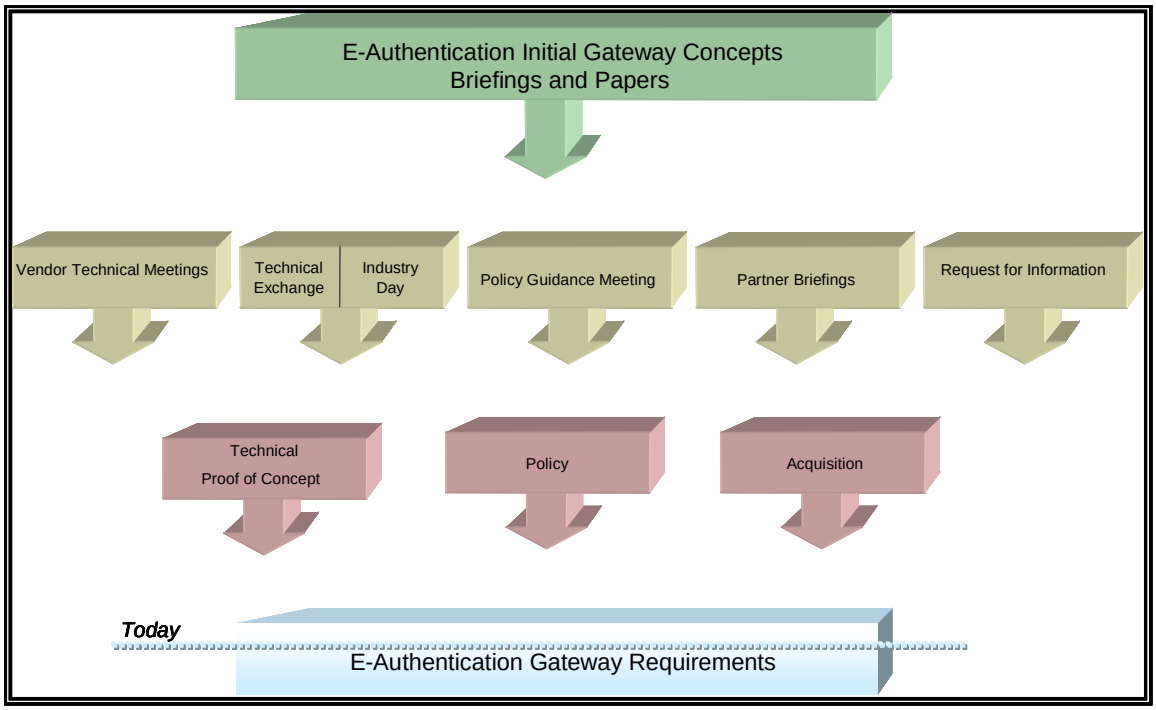


Figure 1.1-2. Interim e-Authentication Gateway Requirements Development Process

At the same time, the Office of Management and Budget (OMB) began the process of defining e-Authentication Guidance for Federal agencies.

The Interim e-Authentication Gateway development team configured and installed commercial-off-the-shelf (COTS) gateway product suites and began testing with government applications as part of an on-going technical proof-of-concept.

The technical meetings, open forums, agency partner briefings, RFI, development of the technical proof-of-concept, guidance, and acquisition strategy are all inputs to the development of the Interim e-Authentication Gateway Requirements definition.

1.2 Purpose and Scope of this Document

The purpose and scope of this document is to describe the operations of the Interim e-Authentication Gateway from the perspective of the user, application and electronic credential provider, in addition to the internal gateway operations.

The definitions and descriptions contained in this document are intended to be concepts representing the goals and functional principles of the Interim e-Authentication Gateway initiative. The interim e-Authentication Gateway is a research and development effort for the purpose of discovering interface, interoperability, and agency technical challenges. These descriptions should not be mistaken for the planned design of the production system that the Government will seek from industry in the future.

The following topics will be addressed in this document:

- The high-level e-Authentication Gateway architecture
- The operations of the Interim E- Authentication Gateway
- Government agency, electronic credential provider, and user interfaces to the Interim e-Authentication Gateway
- Roles and responsibilities for each party

The main portion of this document addresses the above topics as part of the Interim e-Authentication Gateway concept of operations. There are appendices to this document that address additional topics related to the Interim e-Authentication Gateway. They are as follows:

- Appendix A: Technical Context Definitions
- Appendix B: Glossary of Terms

Interim e-Authentication Gateway
In addition, the following two companion documents directly affecting the e-Authentication Initiative are currently under development.

- *E-Authentication Guidance*, under development by OMB
- *E-Authentication Technical Guidance*, under development by National Institutes of Standards and Technology (NIST)

All publicly available information and documentation relating to the e-Authentication initiative can be found at http://www.cio.gov/eauthentication.

1.3 Assumptions

This document assumes that the reader of this document is a member of an agency or commercial entity interested in the e-Authentication initiative and its functional relationship with other e-Gov initiatives and the public consumer.

The concepts of operation described in this document are based on the current operation of the Interim e-Authentication Gateway. Another concept of operations document may be required that relates more specifically to the Government's planned acquisition process.

Roles and responsibilities described in this document reflect the Government's intent to specifically separate identity authentication and access and privilege management. The Interim Gateway provides authentication services to agency applications requiring authentication of users. Agency applications each manage all access controls and privileges associated with the authenticated identity of the user.

The FirstGov Portal (in conjunction with USA Services) may provide user's with the opportunity to configure personal interfaces that contain private information, the usage of which is under the user's control. The Interim e-Authentication Gateway will not be maintaining any individual user private or personal information.

This document assumes the reader has a basic and/or working understanding of technologies related to identity authentication and authorization, such as Public Key Infrastructure (PKI) and privilege management. Appendix C, Glossary, contains definitions of acronyms, abbreviations, and general terms relating to identity management, authentication, and access control technologies.

1.4 Provision of Services

General Services Administration (GSA) is authorized to provide goods and services to the entire Federal government. The GSA has statutory authority to provide Information Technology (IT) and E-Gov services, such as those contemplated for the E-Authentication initiative, to the Federal government. Similarly, GSA established the Access Certificates for Electronic Services program (ACES) for PKI services and Common Access Card (CAC) program for smart card services, under this statutory authority. These service offerings are available through government-wide contract awards. These contracts provide for the issuance of identity credentials to Federal employees and to the public. GSA established the legal structure for these services through legally binding contracts with third-party service providers. In addition, other agencies with more limited authorities have potentially suitable services for segments of users, which will be leveraged, to the extent possible. GSA intends to provide Interim e-Authentication Gateway services through contract(s) with one or more third-party service providers.

The protection of privacy and private information is a primary policy objective for the Gateway and e-Authentication services. It is contemplated that the Interim e-Authentication Gateway would not collect or maintain personal information. The Federal government will ensure that the Gateway and the e-Authentication services are used only for their intended purposes. The Gateway and other e-Gov services and infrastructure will comply with and support the OMB Federal information privacy standards, requirements and guidelines for e-Government.

2.0 Interim e-Authentication Gateway Functionality

2.1 Overview

The Interim e-Authentication Gateway will provide common authentication services and single sign-on capability for all e-Gov applications. The goal is to provide common shared services that all Federal agencies can use to authenticate all users (both internal Federal and external private and public) for all applications that require authentication.

For the purpose of assisting GSA in defining the requirements, implementation issues and interoperability challenges of a fully operational gateway, and to alert and assess the authentication supplier marketplace, an operational interim gateway was deployed October 1, 2002, with full production planned for September 2003.

2.2 Purpose of the Gateway

The primary purpose of the Interim e-Authentication Gateway is to eliminate the need for each of the e-Gov initiatives, as well as other initiatives across Government, to develop and maintain separate services for authentication of users and applications. The Interim e-Authentication Gateway will deliver common interoperable solutions optimizing and leveraging the effort across Government. It will also allow the government to leverage some of the existing electronic credentials and credentialing services already deployed by government and commercial organizations.

Another purpose of the Interim e-Authentication Gateway is for research and development (R&D) of new and emerging gateway and authentication technologies (including interoperability and emerging standards), as part of the development of a set of requirements relating to the planned acquisition of production gateway services.

2.3 Gateway Services

Initially the Interim e-Authentication Gateway will be scaled as an interim service. Agencies that are part of the President's Management Council and identified as an e-Gov Initiative (see Section 1) and other e-Government applications have been authorized to use the Interim e-Authentication Gateway. Ultimately, all agencies with e-Government processes requiring authentication will be able to use the Interim e-Authentication Gateway . Appendix B provides a description of how an agency application is integrated with the Interim e-Authentication Gateway.

2.4 Types of Electronic Credentials Accepted

Each e-Gov application owner will have specific authentication of identity requirements. These requirements correspond to the sensitivity, integrity, and confidentiality of the data and the non-repudiation of the parties involved.

OMB is in the process of developing guideline documents to assist application owners. These guidelines will define several "levels of assurance" that relate to the process of verifying identity as part of the electronic credential issuing process. NIST is in the process of developing a companion document that will define technical components that can be associated with the level of assurance definitions. (see http://www.cio.gov/eauthentication).

The Gateway will accept and validate multiple forms of electronic credentials, issued by multiple Electronic Credential Providers (ECPs), including but not limited to Public Key Infrastructure (PKI) digital signature certificates, Pin and Passwords (P/P, and knowledge-based credentials. This will require that the Interim e-Authentication Gateway have the ability to support multiple authentication and validation protocols to ensure the current validity of the identity credential being presented.

Currently, the e-Authentication Project Management Office (PMO), in conjunction with the agency application owners and OMB, determines the acceptability of electronic credential providers to be integrated with the Interim e-Authentication Gateway. The establishment of an industry-government organizational entity and process to determine the acceptability and trust of different forms of credentials is planned.

2.5 Users

The following are the primary "users" of the Interim e-Authentication Gateway:

- Members of the general public, public businesses, and federal employees. Initially, the number of these users may be limited, at least until the full scalability of the Gateway is assured.

- Government applications are users of the Interim e-Authentication Gateway for the purpose of obtaining authentication services.

- Other users of the Interim e-Authentication Gateway can be defined as internal to the maintenance and operation of the services according to defined roles and responsibilities.

2.6 Interim Gateway Participation

During the interim phase, the Interim e-Authentication Gateway will be used to support the Federal e-Gov initiatives and other e-Government systems that require authentication services.

Currently the e-Authentication PMO, in conjunction with the application owners and OMB, determine the feasibility and applicability of the agency applications integration with the Interim e-Authentication Gateway.

2.7 Gateway Architecture

Figure 2.7-1, The Authentication Gateway, depicts a high level schematic of how the Interim e-Authentication Gateway works. The Gateway is Internet based and links directly to FirstGov, the web-based portal to the Federal government.

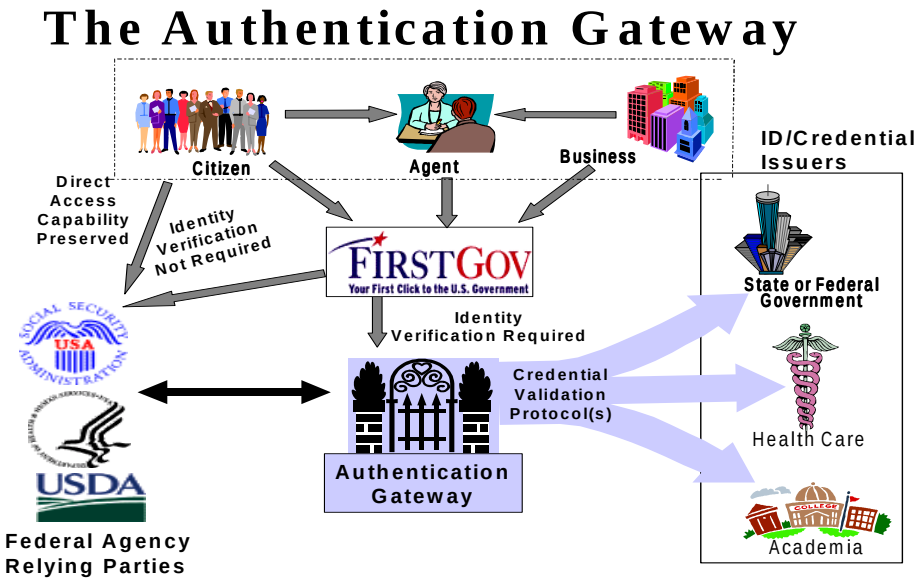


Figure 2.7-1. The Authentication Gateway

2.8 Gateway Core Principles

The Gateway's core principles are:

- The Interim e-Authentication Gateway will not issue credentials. Credentials will be issued by authorized Electronic Credential Providers (ECPs).
- The Interim e-Authentication Gateway accepts electronic credentials from individuals and applications (users) requesting services from e-Gov applications and determines the validity of the credential presented.
- The e-Gov applications are responsible for managing all access controls and permissions related to the services being requested by the users.
- The e-Gov applications are responsible for determining their requirements for unique user information to manage access controls and permissions.

- Each e-Gov application owner will define specific authentication of identity requirements based on the defined levels of assurance in the OMB and NIST guideline documents (see http://www.cio.gov/eauthentication)

- The application may request additional information from the user requesting services in order to grant access. An application may grant access at a higher level of assurance than that associated with the user's credential for use with that local application only. This does not change the level of assurance for the user's credential when access and services from another application are requested by that user.

- Applications requiring lower levels of assurance for authentication of identity will grant access based on validation of credentials issued at a higher level of assurance.

- Once a user's credential has been validated by the Interim e-Authentication Gateway for access to one e-Gov application, access to another e-Gov application will not require re-validation of the credential, if the authentication of identity requirements for the second application are equal to or less than those of the first application (e.g., single sign-on), taking into account timeout and refresh policies.

- The e-Authentication Gateway handles Private Consumer Information (PCI) in accordance with OMB Privacy Management Guidelines. The definition and implementation of the PCI Gateway function of the e-Authentication Gateway will be based on those guidelines.

3.0 Concept of Operations

This section provides functional principles of the Interim e-Authentication Gateway as related to the user, portal, agency application, ECP, and the Interim e-Authentication Gateway itself.

Appendix A, Technical Context Definitions, contains detailed descriptions of the various components used to illustrate the operational principles.

Figure 3.0-1, Interim e-Authentication Gateway Scope, demonstrates the functional scopes of the e-Authentication Interim Gateway and the Agency Applications.

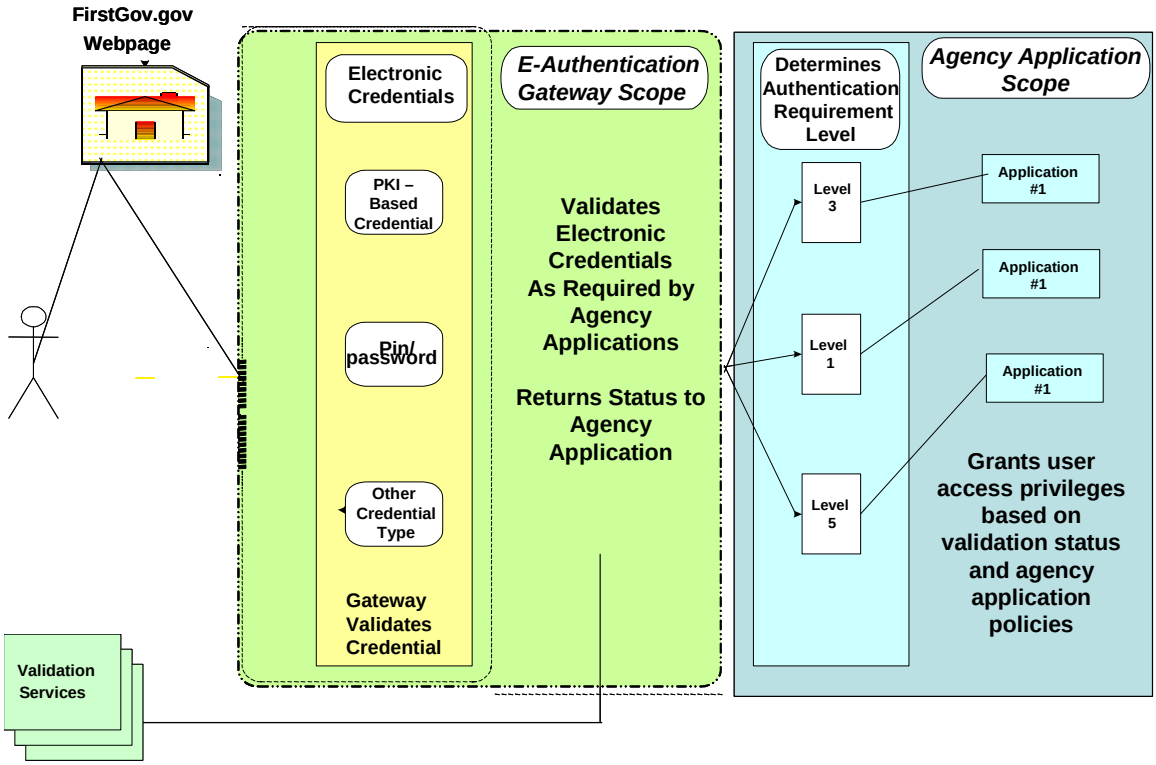


Figure 3.0-1. Interim e-Authentication Functional Scope

- The front-end interface of the Interim e-Authentication Gateway provides a uniform communication interface for agency applications, portals, and users. The back-end interface handles communications with validation services. It is also expected that the gateway will be able to communicate via the many disparate communication protocols required by the validation services.

- If a user accesses the agency application directly, the application has the option of validating the user's credentials using its own authentication processing or by using the Interim e-Authentication Gateway to validate the credentials.

- The scope of the gateway is specific to authentication only of user credentials on behalf of agency applications. Agency applications manage permissions and all access controls (authorization) for their systems.

- Once the user has been authenticated by the Interim e-Authentication Gateway for access to one agency application, the user may or may not be required to re-authenticate at another agency application using the gateway, based upon policies relating to "session" management.

- Electronic credential levels and credential mechanisms are explicitly separated technologically. The level of assurance associated with an electronic credential

may be a cardinal value or an algorithmic score. There are a number of electronic credential presentation mechanisms, such as personal identification number (PIN) and passwords (including one-time passwords),PKI-based (including X.509v3 certificates), and knowledge-based credentials.

- A user may have multiple digital credentials, at the same or different levels. If the user obtains higher level credentials, the lower level credentials are still useable where appropriate.

- If a user has no digital credentials, the Government will provide information on credential requirements and will maintain a list of authorized ECPs that offer digital credentials at the appropriate or higher level.

- Support for validation of credentials to support anonymous and pseudonymous access to agency applications is also expected.

3.1 User Operational Concepts

This section provides a summary of the Interim e-Authentication Gateway operational concepts from the individual member of the public or business user's perspective:

- The user can access agency applications directly, via the portal as a set of web links, or via the portal as a "proxy" login for agency applications.

- The user will need to allow the creation of "cookies" (non-persistent) in their web browsers to support a one-time authentication across multiple agency applications (single sign-on).

- The user session (if cookies are allowed) will continue until the browser is closed, until it is timed-out (for inactivity and/or time at the application or gateway), or the user explicitly logs out.

- The user can have multiple credentials of various levels of assurance for the same role-based identity.

- If the user has no credentials or access to an agency application requires a different level of assurance credential, the user may be redirected to obtain another credential of their choice or the application may request additional information from the user and grant a "temporary" upgrade to their credential for that application only.

- If the user does not permit cookies to be created, authentication and re-authentication will be required for access to each agency application requested (no single sign on).

3.2 Portal Operational Concepts

The following section contains a summary of the Interim e-Authentication Gateway operational concepts from the perspective of the portal:

- The FirstGov portal will be the first point of entry for the user seeking agency application services.
- The portal will provide a list of services available and the authentication requirements associated for granting access to those services.
- The portal will provide information to users about electronic identity credentials and where and how to obtain them.
- The portal may provide a "proxy" login for the user and maintain session management through the issuance of non-persistent cookies
- The portal may provide information to the user about the opportunity to set preferences for future access with Government services.

3.3 Agency Application Operational Concepts

The following is a summary of the Interim e-Authentication Gateway operational concepts from the perspective of the agency application:

- The agency application determines authentication level requirements for all of its protected resources.
- The agency application may be the first point of entry for the user seeking services.
- The agency application may request the user to present credentials to be authenticated.
- If the agency application is also the user's ECP, the credential may be validated by the agency application or the application may utilize the Interim e-Authentication Gateway to validate the user's credential.
- The agency application determines and maintains authorizations, access controls, and user privileges related to protected resources.

3.4 Electronic Credential Provider (ECP) Operational Concepts

The following is a summary of the Interim e-Authentication Gateway operational concepts from the perspective of the Electronic Credential Provider (ECP):

- The ECP provides user identity management services.

  - Collects and verifies identity information from the user.
  - Issues and manages user credentials.

- The ECP defines the protocols supported for validation of credentials.

- The ECP responds to credential status information/validation requests received from the Interim e-Authentication Gateway and/or agency applications.

3.5 Gateway Operational Concepts

The following is a summary of the Interim e-Authentication Gateway operational concepts from the perspective of the Interim e-Authentication Gateway:

- The gateway provides user login for agency applications.
- The gateway maintains information regarding agency application requirements for authentication (e.g., identity authentication level of assurance information).
- The gateway requests credentials for validation from the user.
- The gateway may respond to requests for validation of user credentials received from the agency applications.
- The gateway issues a request for validation of a user's electronic credential from the ECP that issued it.
- The gateway returns a response type indicating the status of the credential and other user information as required or permitted.
- The gateway manages user sessions and assists the agency applications in session management.
- The gateway does not maintain user personal information or user behavior and profiles.

3.6 Gateway Process Flows

The following sections will describe a typical gateway process flow and two specific process flows, based on the current Interim e-Authentication Gateway Architectures.

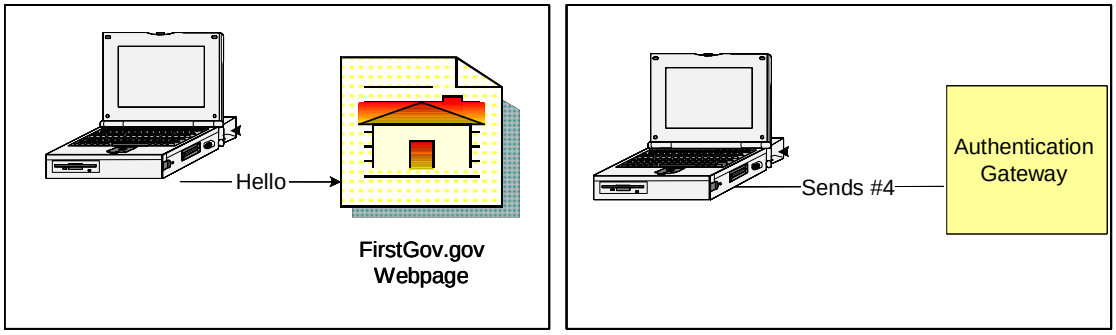
3.6.1 Typical e-Authentication Process Flow Concept

Figure 3.6.1-1, Typical e-Authentication Process Flow Concept, illustrates a typical Interim e-Authentication Gateway user session at a high level. It assumes that the user initially discovers the desired e-Gov application via a portal, such as FirstGov.gov:

Step 1: A user comes to the FirstGov web portal:

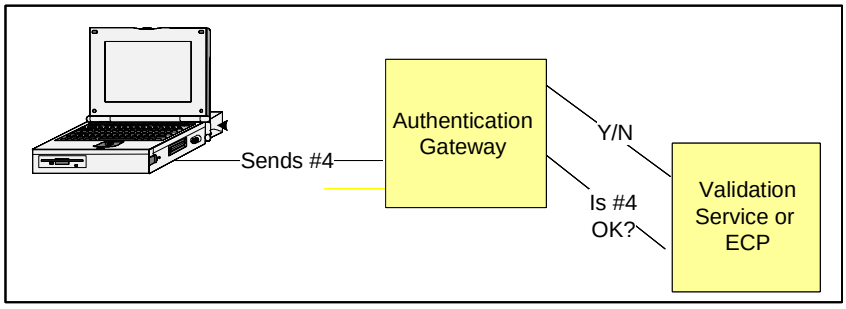
- At the portal, the user selects an e-Gov application such as one from United States Department of Agriculture-National Finance Center (USDA-NFC).

- Before the user begins interacting with the application, the portal queries the Interim e-Authentication Gateway for USDA-NFC's authentication level of assurance requirements (e.g., must be Assurance Level 4 in the example). (The gateway retrieves the authentication level requirements from decentralized lists and databases.)

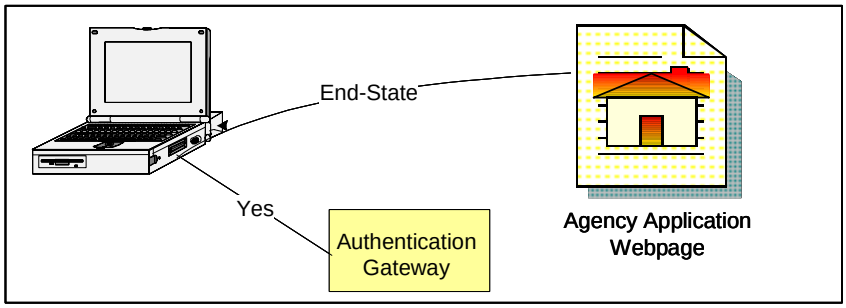


Step 1. User goes to FirstGov web portal and selects e-Gov application service

Step 2.. User is re-directed to e-Authentication Gateway to present credential required by application.



Step 3. e-Authentication Gateway validates user's credential



Step 4. If user's credential is valid, user is re-directed to agency application for services

Figure 3.6.1-1. Typical e-Authentication Process Flow Concept

Step 2: Based on the application and service selected by the user:

- The gateway queries the user for a credential matching or exceeding the required level
- The user's credential is presented to the gateway.
- If the user does not have a digital credential of the appropriate level, the user is denied access to the application and re-directed back to the portal for further information.

Step 3: The user's credential is validated:

- The Interim e-Authentication Gateway validates the user's digital credential via a validation service or by performing a query directly to the ECP.
- If the digital credential is valid, the Interim e-Authentication Gateway's response to this effect is conveyed to the application and the user's browser is updated with a non-persistent cookie.
- If the credential is not valid, the user is informed that their digital credential has been rejected and is provided with a link to be re-directed to the web portal.

Step 4: If the credential is valid, the user is re-directed to the agency application to obtain desired services.

After the user has been initially authenticated by the Interim e-Authentication Gateway, the user may select another application. The other application will query the Interim e-Authentication Gateway for session and validation information and proceed to grant access to the user, according to its own access controls and privilege management policies. The user will not have to be re-authentication if this occurs.

3.6.2 Interim e-Authentication Gateway Architecture and Process Flow 1

Figure 3.6.2-1, Interim e-Authentication Gateway Architecture 1, illustrates a gateway architecture that demonstrates the implementation of a closed, proprietary system designed to support a particular set of agency applications. This architecture supports validation of username/password and PKI credentials.

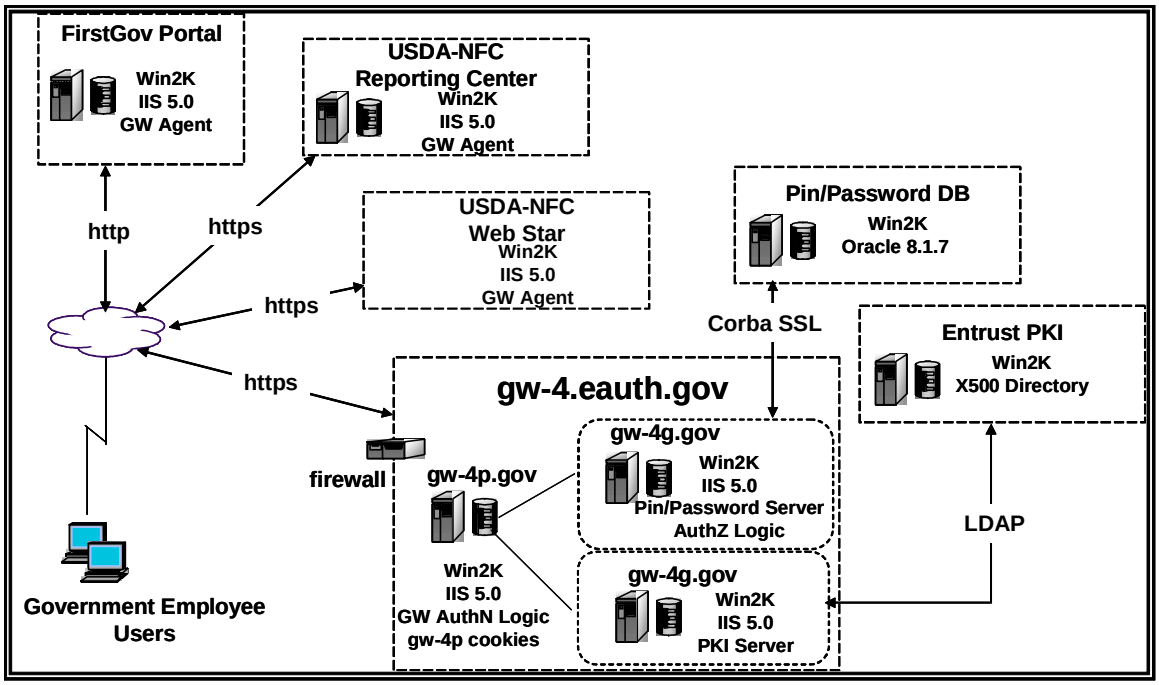


Figure 3.6.2-1. Interim e-Authentication Gateway Architecture 1

Figure 3.6.2-2, On-Line Interim e-Authentication Gateway System Process Flow 1, illustrates the following process flow scenario:

Step 1: User initiates activity at the FirstGov portal:

Step 2: Portal challenges the user for login and credential.

- User selects one a type of credential, [i.e., pin/password, PKI X.509 certificate].

- User's browser provides the credential to the gateway for validation.

Step 3: The Gateway validates the credential

- If the credential is valid, issues a "non-persistent" cookie to the user's browser.

Step 4: The user is then presented with a list of applications available, based on the credential validated. If the PKI certificate was validated, the user will have more applications to chose from.

- The user selects application.

Step 5: The application checks the gateway for status of the user session.

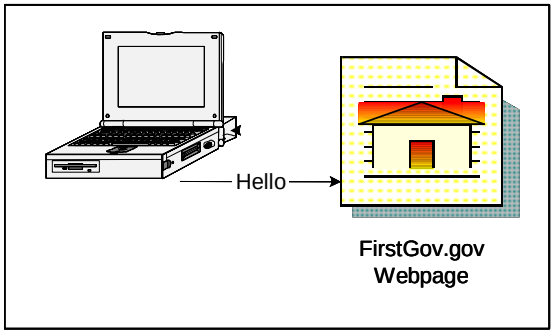
- If the session is valid, the application issues a non-persistent cookie to the browser or updates a current cookie.

- The user is granted access.

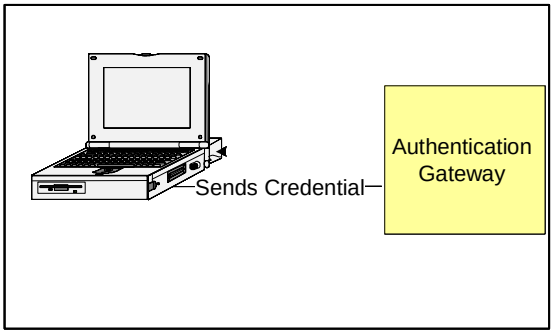
Step 6: User selects a second application either from the portal or the browser list.

- The application checks with the gateway for status of user session and credential status.

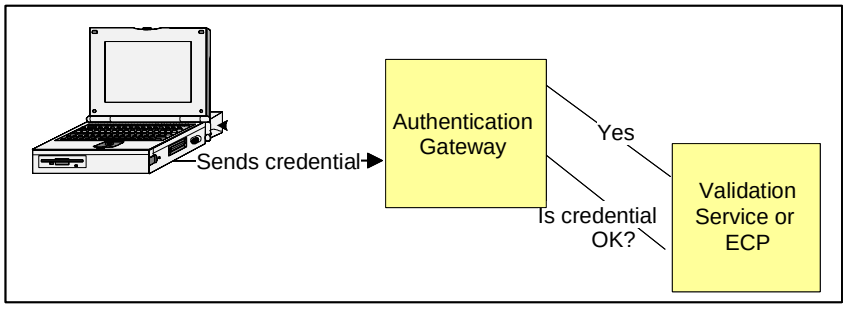
- If the second application requires a PKI certificate credential and the user has been validated for a PKI certificate credential, the



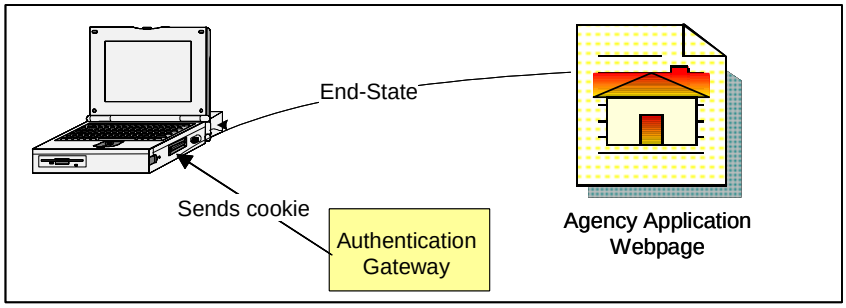
Step 1. User goes to FirstGov web portal



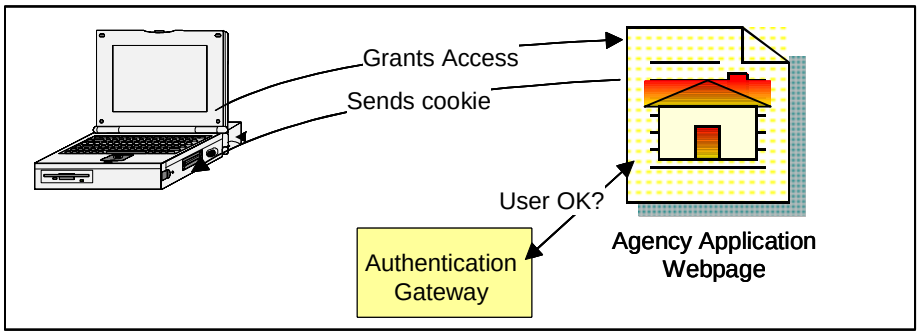
Step 2.. Portal challenges user for login and credential



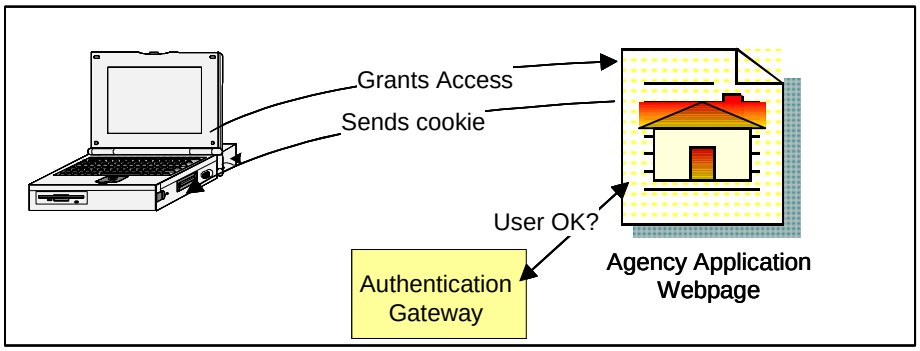
Step 3. e-Authentication Gateway validates user's credential



Step 4. If user's credential is valid, gateway sends user's browser a non-persistent cookie and user is re-directed to agency application to select service from a list of services, based on credential validated



Step 5. Agency application checks user's status with the gateway, sends non-persistent cookie, and grants access



Step 6. User selects second application. Application checks user's status with the gateway, sends non-persistent cookie, and grants access if credential meets requirements

Figure 3.6.2-2. On-Line Interim e-Authentication Gateway System Process Flow 1

3.6.3 Interim e-Authentication Gateway Architecture and Process Flow 2

Figure 3.6.3-1, Interim e-Authentication Gateway Architecture 2, illustrates a gateway architecture that demonstrates the implementation of the Security Assertion Markup Language (SAML) proposed open standard protocol. This architecture supports validation of username/password and PKI credentials.

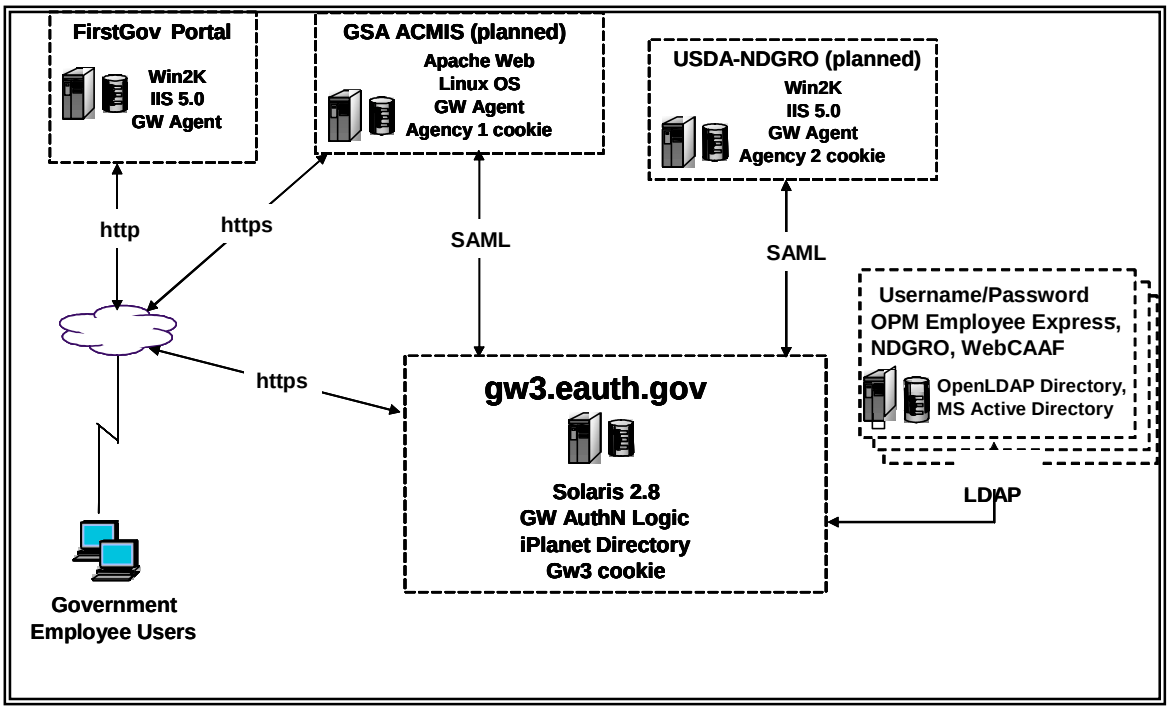


Figure 3.6.3-1. Interim e-Authentication Gateway Architecture 2

Figure 3.6.3-2, Interim e-Authentication Gateway Process Flow 2, illustrates the following process flow scenario:

Step 1: User goes to FirstGov portal and selects the desired agency application

- User selects desired resource (web page) at agency

Step 2. The Policy Enforcement Point at the agency application sees that the user has not yet logged in and automatically redirects the user's browser to the login page at the Interim e-Authentication Gateway

- The user presents their electronic credentials (e.g., pin/password or PKI certificate) to the gateway

Step 3: The gateway validates the user's credential

- The gateway queries the issuing ECP as to the validity of the electronic credentials. The ECP responds that the electronic credentials are still valid.

Step 4: The gateway sets a non-persistent cookie in the user's browser indicating that the user has successfully logged into the gateway.

- The gateway also sets a SAML artifact in the Uniform Resource Locator (URL) query string. SAML artifacts are 42 bytes long, consisting of a 2-byte artifact type code, a 20-byte source ID which uniquely identifies the issuing a "source site" (the gateway in this example), and a 20-byte assertion handle which is a cryptographically

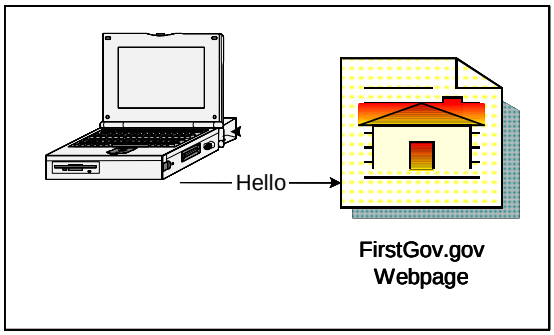
strong random or pseudorandom number sequence which is an ephemeral handle that uniquely identify the user for *this single agency application/gateway transaction only*.

Step 5: The agency application checks the SAML artifact with the gateway

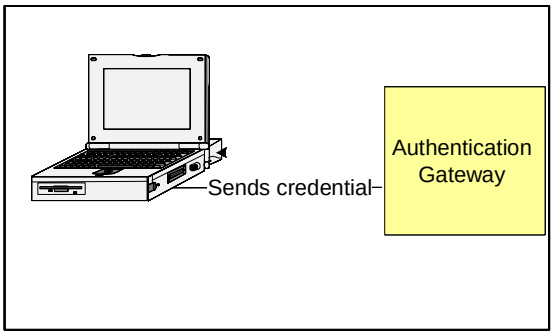
- The user's browser is re-directed to the agency application SAML consumer, which extracts the SAML artifact and passes that in an encrypted tunnel (e.g., via HTTPS) to the gateway.
- The gateway replies with a SAML assertion referenced by the SAML artifact. The gateway is required to check that the artifact is coming from the expected agency application, otherwise it is to respond with an empty assertion. The gateway is also required to implement the "one-use" artifact policy; i.e., future requests using the same artifact will result in an empty SAML assertion.
- The SAML assertion contains additional information (e.g., user name, issuing ECP, customer number, etc.) about the user who was authenticated by the gateway.
- The agency application then sets a non-persistent cookie to indicate the session state. At this point the user has successfully logged into to both gateway and agency application and is granted access to the agency application.

Step 6: Next, the user selects from their browser's "favorites" list a URL on a different agency application. Also assume the user has not visited that application today (i.e., during this gateway session), and therefore lacks a non-persistent cookie from that agency application indicating a previously successful login.

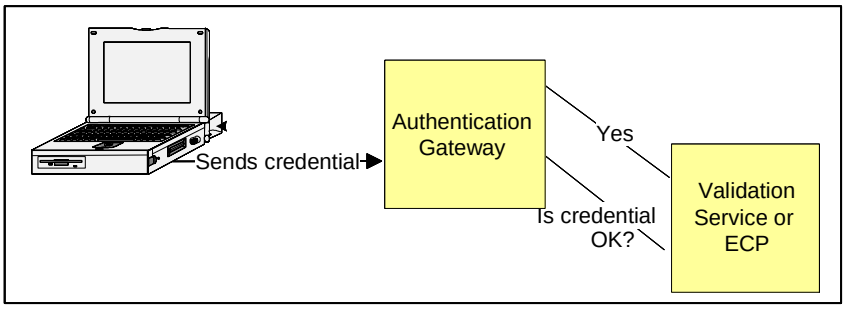
- The user is redirected to the login page on the gateway. However, the gateway sees the cookie it set for itself indicating that the user has previously (during this gateway session) successfully authenticated themselves to the gateway. Therefore, the user is not prompted for their electronic credentials.
- The gateway automatically redirects the user's browser to the SAML consumer on the second agency application, passing with it a new, different SAML artifact. The second agency application then sends that SAML artifact to the gateway.
- The gateway responds with the SAML assertion corresponding to that SAML artifact. The second agency application then sets a non-persistent session cookie for itself while automatically redirecting the user's browser to the second desired URL.



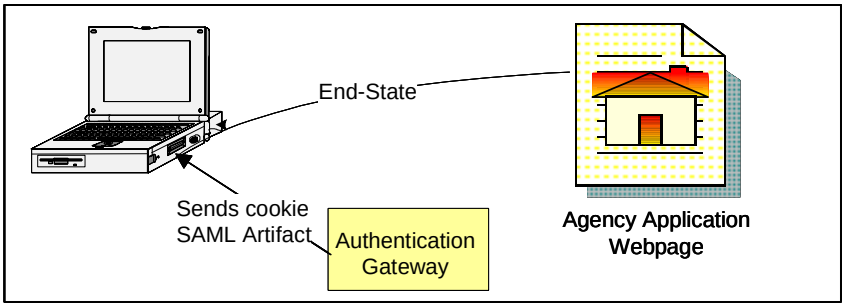
Step 1. User goes to FirstGov web portal and selects e-Gov agency application service



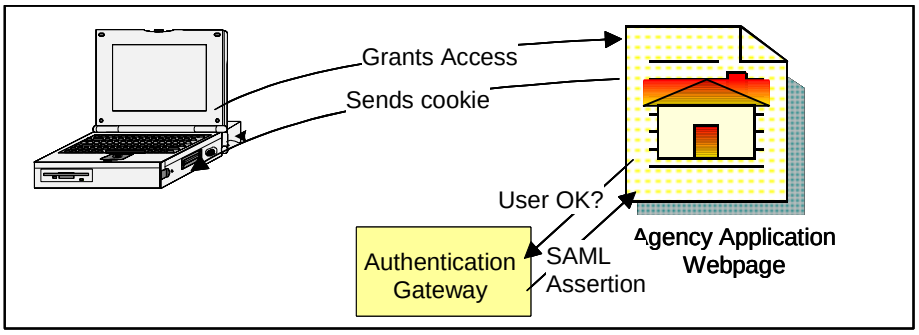
Step 2.. User is re-directed to e-Authentication Gateway by agency application to present credential required by application.



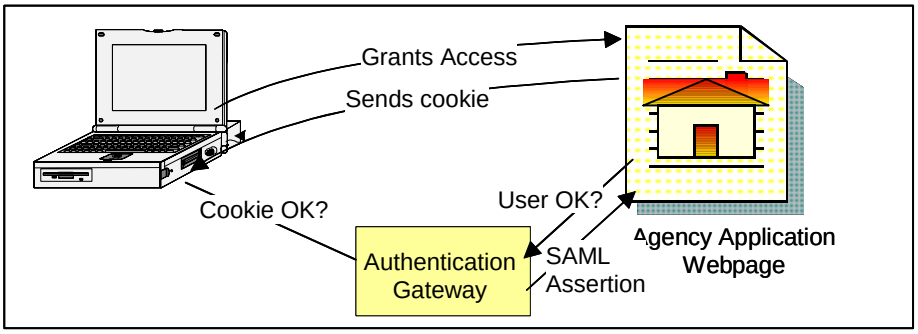
Step 3. e-Authentication Gateway validates user's credential



Step 4. If user's credential is valid, gateway sends user's browser a non-persistent cookie and SAML artifact and user is re-directed to agency application SAML consumer



Step 5. Agency application checks SAML artifact with gateway and the gateway returns the correct SAML assertion. Agency application sends non-persistent cookie and grants access.



Step 6. User selects second application from their browser and is redirected to the gateway. Gateway checks the user's cookie and redirects user to second application. Application checks SAML artifact with gateway and the gateway returns the correct SAML assertion. Agency application sends non-persistent cookie and grants access.

Figure 3.6.3-2. Interim e-Authentication Gateway Process Flow 2

3.6.4 Interim e-Authentication Gateway Session Management

The e-Authentication Gateway maintains a session state for itself; this is the "single sign-on" state for all of the e-Authentication gateway participants. Per suggestions in the SAML specification, it is also assumed that each agency application has a "security engine" that will also maintain its own login state. This allows each user, once authenticated by the e-Authentication Interim Gateway, to repeatedly interact with the agency application (during that session) without being redirected to the gateway. Therefore, there is one session state for the gateway and one session state for each agency application visited by the user.

Session state may be maintained via non-persistent cookies. From the perspective of the gateway or an agency application, a gateway session ends when the user accesses the "logout" button, by closing the browser, or when the maximum session lifetime value (e.g., 4 30 minutes, 3 hours to 8 hours1 day) is exceeded.

3.6.5 Cookies

Only non-persistent cookies are used, i.e., cookies that are not stored on the user's hard disk and cookies that are deleted from memory when the user's browser is closed.

Cookies do not contain any directly Personally Identifiable Information (PII). Cookies may, however, contain an ephemeral index number that the Interim e-Authentication Gateway or an agency application can use to access PII. However, the ephemeral index number must be unique for each Interim e-Authentication Gateway or agency application session.

3.6.6 Interim e-Authentication Gateway Product Testing

Following the initial identification and definition of Interim e-Authentication Gateway high-level functional requirements, the Interim e-Authentication Gateway Development Team initiated a series of meetings with interested gateway Commercial-Off-The-Shelf (COTS) product representatives. These meetings are conducted as an ongoing activity, for the following purposes:

- To establish and maintain a knowledge base of the current state-of-the-art in the marketplace.

- To establish and maintain a cooperative relationship between Government and industry as part of the R&D effort.

- To define and represent the Government's specific and unique requirements to industry.

The initial on-line interim gateway system was designed to meet the unique and proprietary needs of the first agency application interoperability testing partner, as a first demonstration of the "Proof-of-Concept."

The second on-line interim gateway system was designed to demonstrate and alternative architecture that could represent a more open system, standards-based approach.

It should be noted that the current state-of-the-art in the marketplace does not support interoperability between gateway core products and/or agency application web server agents.

4.0 Agency Application Interoperability

The following sections summarize the process for agency applications to interoperate with the Interim e-Authentication Gateway.

4.1 Authentication Requirement Levels

The agency needs to assess the level of risk it is willing to assume in determining the authentication of identity. The level of assurance of a digital credential is the degree of confidence in the binding of the identity to the credential issued. The documents being developed by OMB and NIST will provide guidance in this process.

Additionally, the E-Authentication team can provide an assessment tool, called e-RA, to assist agencies in undertaking risk assessments.

Following the determination of level of risk, the agency can determine the required level of assurance for the application.

The Interim e-authentication Gateway will then validate user credentials, based on the agency's level of assurance requirement.

4.2 Agency Support for Validation of User Credentials

The Interim e-Authentication Gateway queries credential-issuing entities to validate the users credentials. If the Federal agency has issued the credentials (e.g., is an ECP), the Agency's database or repository will need to provide access to the gateway for validation of the credentials it has issued.

4.3. Agency Application Interfaces

The Interim e-Authentication Gateway supports a uniform interface(s) and defined protocols for interfacing with agency applications. Protocols will include presenting the information concerning the authenticated user in a standard way for the agency applications to accept that information.

An agency application web server is protected by installing a vendor-specific ISAPI, NSAPI, or Apache module plug-in. A vendor specific module is installed on every physical device (web server application) that has a unique IP address and only one vendor specific module can be installed on a web server. That module interfaces with a single specified gateway.

When the web server starts (or is restarted) it reads the resource protection policies from a remote policy store (LDAP directory) located at the Interim e-Authentication Gateway. Using this method, code does NOT have to be integrated into each web page being protected. The resources to be protected are designated by a separate policy GUI and are stored in the policy store.

The following is a list of the "known good configurations" for agency application web servers to interface with the gateway:

- Known good configurations
  - Win2K w/ SP2, running IIS 5.0
  - Sun's JRE v1.3.1_02 is also needed if
    - SAML support is desired, or
    - An EJB application server, JSP servlet engine/container (web service) is being protected
- Typically do NOT want Sun's standalone J2EE (containing Sun's standalone JVM); instead, want Sun's J2SE
- All products reported support for configurations on SPARC boxes (but none have been successfully tested to date)
- Interface from gateway web agent to backend business processes for access controls is customized per application

4.4 Agency Application Interoperability Testing

Following the agency application determination of authentication requirements, their technical integration team met with the Interim e-Authentication Gateway technical team. The purpose of these meetings is to identify unique interoperability requirements and to determine integration requirements to complete interface from agency application gateway module to backend business processes.

The agency application will need to structure their web server to protect resources in accordance with agency authorization management policies.

4.5 Interim e-Authentication Gateway/Agency Application Authorization to Interconnect

Following completion of integration testing with gateway development testbed, integration with the appropriate "on-line" gateway product will be completed, once authorization by the e-Authentication PMO has been issued.

The e-Authentication PMO will determine that the agency application has performed due diligence in addressing Federal and agency regulations regarding security and risk mitigation strategies. The e-Authentication PMO will also determine that the Interim e-Authentication Gateway has addressed the same issues related to interconnection with the agency application.

The final step is the completion of the Memorandum of Understanding or Relying Party Agreement by both the agency application and the e-Authentication PMO. The agency application and the Interim e-Authentication Gateway will then be authorized to interconnect.

5.0 User Gateway Interfaces

For individual user's, the primary interface to the Interim e-Authentication Gateway will be via the FirstGov.gov portal or the agency application from which the user is requesting services, using an Internet web browser software application. For business process-to-business process "users," the interface will be an agreed upon protocol.

5.1 User Credentials

The Interim e-Authentication Gateway does not issue credentials. In some cases, the agency will be the ECP. In other cases, a trusted third-party will be the ECP.

In those cases, where the user does not have credentials, the FirstGov.gov portal and/or the agency application will provide the user a list of approved ECPs. The FirstGov.gov portal and/or the agency applications will convey to the user the level of assurance related to the authentication of identity required for access to the agency applications. The user may go to one of these ECPs to obtain the appropriate electronic credential.

If an individual requires an electronic credential with a higher level of assurance to transact business, they may be required to have new credentials issued to meet that higher requirement or provide the agency application with additional identity information.

An identity assurance that permits access at a higher assurance level will be accepted by applications requiring lower authentication of identity assurance levels.

5.2 User Data

The Interim e-Authentication Gateway does not maintain user information. It queries appropriate databases for validation of the status of the user's credentials.

Users may be provided an opportunity to establish "personal preferences" or "personal profile information" at the portal, a related portal services, or a third-party service provider. The use of this information by the Interim e-Authentication Gateway or agency application would only be done as defined by the user.

6.0 Electronic Credential Providers (ECPs)

All ECPs will enter into an agreement to provide electronic credential status information to the Interim e-Authentication Gateway for the credentials they have issued. The ECPs specify the protocols they support for providing access to their databases, directories, and/or repositories. The costs associated with providing this service are as agreed between the e-Authentication PMO and the ECP. Funding is centrally provided through the e-Authentication PMO.

The credentials issued by the ECPs will have an associated level of assurance as defined in the policy guidelines documents.

Agency applications will determine the level of assurance they require for their applications and/or specify the ECPs from which they will accept credentials.

6.1 ECP Interfaces and Interoperability Testing

Although there are potentially an infinite number of ECPs, each one requiring unique protocol and network communication interface specifications, the following are the current primary types and processes supported for interoperability testing:

- PIN & Password
    - User's login name is used to determine the full distinguished name (DN) to their record
    - A "bind" is attempted to the directory using the supplied password
    - Resulting pass/fail status of that bind attempt determines the status of the supplied password
        - iPlanet LDAP directory generally supported
        - OpenLDAP supported by at least one product
        - Users should be installed in a general, well-known directory schema
- PKI-based
    - Most products assume a client-side SSL certificate is being used for user identification
    - Web servers typically complete SSL tunnel setups before the ISAPI, NSAPI, or Apache module (which protects the web resources) is called
    - Generally assumed that the target web site validates the certificate before the gateway-specific enforcer is called
    - Interim e-Authentication Gateway supports LDAP for Certificate Revocation List (CRL) retrieval and Online Certificate Status Protocol (OCSP) validation protocols
    - The Interim e-Authentication Gateway also supports the Certificate Arbitration Module (CAM) / Discovery and Validation Engine (DAVE) custom validation protocol.

Currently, candidate ECPs are selected based on agency application specific requirements. The following is a list of the ECPs currently who have completed interoperability testing or are being considered for interoperability testing in the Interim e-Authentication Gateway:

- Internal Government potential ECPs: USDA-NFC, ACES, Treasury-Pay.Gov, Treasury, DoD, NASA, OPM-Employee Express, USDA-WebCAAF

- External Government potential ECPs: State issued credentials (e.g., Illinois), universities, banking industry, healthcare

Appendix A: Technical Context Definitions

1.0 Context Diagram

Figure A1.0-1, Context Diagram, is a pictorial representation of how various entities will interact with the Interim e-Authentication Gateway.

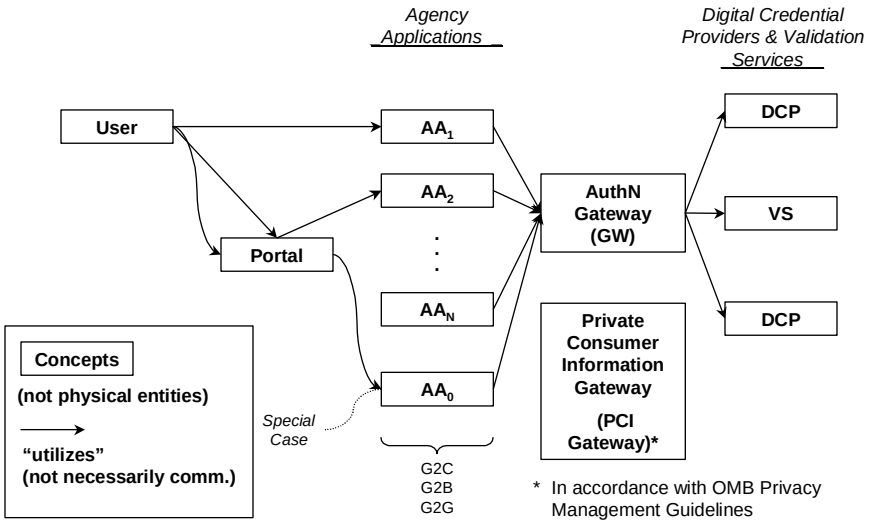


Figure A1.0-1. Context Diagram

The following list defines each of the components in the above diagram:

- **This diagram is not an architecture**
- Blocks represent conceptual roles, not physical entities
- Arrows represent generalized "utilization," not communication
- AA1 thru AAn represent the e-Gov initiatives and other agency applications
- AA0 represents authentication "to the system" (may appear as authentication to the portal to the user) before going to any particular AA
- Concept of AA0 introduced so all "first contact and transfer" scenarios now look similar; don't need special cases for each
- Private Consumer Information (PCI) Gateway has same utilizations as e-Authentication Gateway … lines would make drawing too cluttered
- PCI Gateway concept is introduced to separate discussion of private information policies / requirements because of requirements for specific policies regarding PCI
- A user may access an agency application in the following three ways:
  - Directly
  - By visiting the portal and clicking on a link for the application (The portal may be a government portal or a private portal of a ECP)
  - Via the portal as a proxy to the application, i.e., all communications between the user and the agency application must flow through the portal

Agency applications (AAs) may use the Interim e-Authentication Gateway to authenticate users who access the application directly, rather than through the portal. In that case, AA0 could be used to provide consistent interoperations among the component roles.

- The Private Consumer Information (PCI) Gateway supports the technical capability required to collect, transfer and maintain information during the logging process. Beyond that required for logging purposes, it is not anticipated that there will be private consumer information collected or maintained at or by the gateway.

2.0 Gateway ECP Component Interfaces

Figure A2.0-1, Electronic Credential Providers (ECPs) and Validation Services (VS), illustrates the relationships of the ECP components to the Gateway. As shown, the credentials are issued by the ECP not by the validation service.

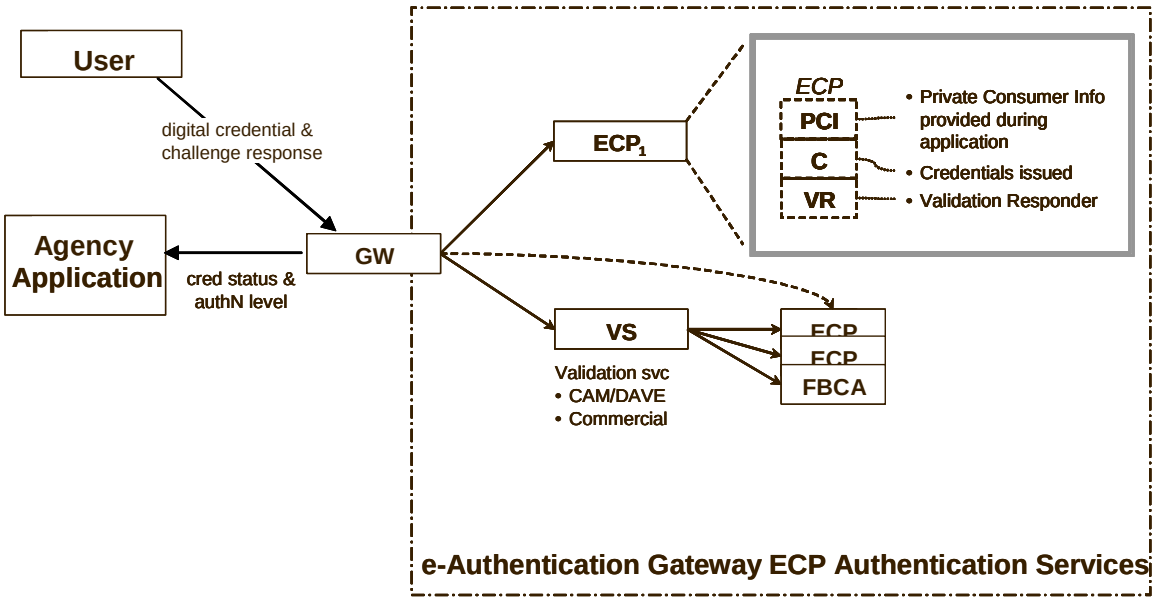


Figure A2.0-1. Electronic Credential Providers (ECPs) and Validation Services (VS)

Figure A2.0-1 illustrates validation of services via direct access to the ECP and via validation services, where the validation service does not actually issue credentials. The curved, dotted line illustrates that the gateway could request validation directly from an ECP, even if the ECP is also a component of a validation service.

These concepts are introduced so they may be considered separately. It illustrates how the authentication via ECPs works internally vs. how it interacts with others.

3.0 Interim e-Authentication Gateway Characteristics

This section defines the primary characteristics of the Interim e-Authentication Gateway:

- Back-end" interface
  - Handles communications with validation responders and validation services
  - Non-uniform communication interfaces
    - Commercial services
    - Legacy agency application accounts
- "Front-end" interface
  - Handles communications with agency applications and/or users
  - Uniform communication interfaces
- Operating logic
  - Understands credential "levels"
  - Has database of agency application credential requirements
  - Manages session state

4.0 Electronic Credential Providers (ECPs)

The following list defines the primary characteristics relating to ECPs, credentials, and the Interim e-Authentication Gateway:

- Credentials come in various authentication (authN) levels
  - "Levels" relate to thoroughness of authentication of identity at issuance "Levels" are not indicative of confidentiality afforded during use (see OMB and NIST guidance documents which can be found at http://www.cio.gov/eauthentication
- Credential presentation methods (decoupled from "level")
  - PIN and password (includes one-time passwords)
  - PKI-based (includes smart cards)
- Types of credentials
  - Issued by agency application that is also an ECP
  - Government issued for Government use only (e.g., ACES)
  - Non-government issued (e.g., commercially issued credentials)
- Agency Applications have known credential requirements
  - May ask user for additional information to temporarily increase them to higher authorization level for that session only or for their own application only

5.0 Gateway Response Types

Following authentication of the electronic credential, the Interim e-Authentication Gateway gives the user one of following signed responses, which the user gives to each agency application it visits)

- Anonymous Ticket (e.g., movie tickets)
    - Contains no user-specific information; used for anonymous access
    - Presence / possession means met some criteria
    - No way for Agency Application (AA) to get additional user info (from ECP or AA)
- Pass (e.g., airline boarding pass)
    - Full, stand-alone payload
        - Contains user's submitted credentials
    - No need for agency application to contact gateway for further information
- Partial Pass (e.g., ACES certificate)
    - Some user-specific information
    - Agency application may need to get additional user info (from ECP or user)
- Voucher
    - Is an index into ECPs or Agency application databases; to be used by agency application to obtain additional desired user info
        - May be ephemeral to prevent unauthorized tracking

Appendix B. Glossary

ACRONYMS AND ABBREVIATIONS

AA_n	An "arbitrary" Agency Application
AAs	Agency Applications
ACES	Access Certificates for Electronic Services
API	Applications Programming Interface
ARL	Authentication Requirements Level
AuthN	Authentication
AuthZ	Authorization
CAM	Certificate Arbitration Module
COTS	Commercial-Off-The-Shelf
CRL	(digital) Credential Revocation List
DAVE	(path) Discovery and Validation Engine
DoD	Department of Defense
ECP	Electronic Credential Providers
FBCA	Federal Bridge Certification Authority
FirstGov	Government wide portal found at www.firstgov.gov
FPKIPA	Federal Public Key Infrastructure Policy Authority
G2B	Government – Business transactions
G2C	Government – Citizen transactions
G2G	Government – Government transactions
GSA	General Services Administration
GW	Gateway
GWAC	Government-wide Agency Contract
IETF	Internet Engineering Task Force
MOU	Memorandum of Understanding
NASA	National Aeronautical Space Administration
NIST	National Institutes of Standards and Technology
OASIS	Organization for the Advancement of Structured Information Standards
OMB	Office of Management and Budget
P/P	Pin and Passwords
PCI	Private Consumer Information
PDA	Personal Digital Assistant
PII	Personally Identifiable Information
PKI	Public Key Infrastructure
PMO	Project Management Office
R&D	Research and Development
RFC	Request for Comment
RFI	Request for Information
SAML	Security Assertion Markup Language
SSA	Social Security Administration
VS	(Digital Credential) Validation Service

DEFINITION OF TERMS

Term	Definition
Access	Ability to make use of any information system (IS) resource.
Access Control	Process of granting access to information system resources only to authorized users, programs, processes, or other systems.
Activation Data	Private data, other than keys, that are required to access cryptographic modules (i.e., unlock private keys for signing or decryption events).
Agency	For purposes of this document only, agency is defined as any instrumentality of the government, federal, state, and local.
Anonymous access	Unidentified access to agency application
Applicant	The subscriber is sometimes also called an "applicant" after applying to a certification authority for a certificate, but before the certificate issuance procedure is completed.
Attribute Authority	An entity recognized by the Federal PKI Policy Authority or comparable Entity body as having the authority to verify the association of attributes to an identity.
Authenticate	To confirm the identity of an entity when that identity is presented.
Authentication	Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information.
Binding	Process of associating two related elements of information.
Certificate	A digital representation of information which at least (1) identifies the certification authority issuing it, (2) names or identifies its subscriber, (3) contains the subscriber's public key, (4) identifies its operational period, and (5) is digitally signed by the certification authority issuing it. .
Certification Authority (CA)	An authority trusted by one or more users to issue and manage X.509 Public Key Certificates and CARLs or CRLs.
Certification Authority Revocation List (CARL)	A signed, time-stamped list of serial numbers of CA public key certificates, including cross-certificates, that have been revoked.

Term	Definition
Certificate-Related Information	Information, such as a subscriber's postal address, that is not included in a certificate. May be used by a CA managing certificates.
Certificate Revocation List (CRL)	A list maintained by a Certification Authority of the certificates which it has issued that are revoked prior to their stated expiration date.
Certificate Status Authority	A trusted entity that provides on-line verification to a Relying Party of a subject certificate's trustworthiness, and may also provide additional attribute information for the subject certificate.
Client (application)	A system entity, usually a computer process acting on behalf of a human user, that makes use of a service provided by a server.
Compromise	Disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred.
Confidentiality	Assurance that information is not disclosed to unauthorized entities or processes.
Cookie	A "cookie" is a small piece of information contained in a text file that is sent by a web server to be stored on a web browser, so that it can later be read back from that browser the next time this visitor returns.
Cryptographic Module	The set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes, including cryptographic algorithms, and is contained within the cryptographic boundary of the module.
Data Integrity	Assurance that the data are unchanged from creation to reception.
Digital Signature	The result of a transformation of a message by means of a cryptographic system using keys such that a Relying Party can determine: (1) whether the transformation was created using the private key that corresponds to the public key in the signer’s digital certificate; and (2) whether the message has been altered since the transformation was made.
E-commerce	The use of network technology (especially the internet) to buy or sell goods and services.

Term	Definition
e-Gov Application	Any government application establishing an electronic interface to users for doing business with the government application
e-Gov Initiative	e-Gov application that is identified as part of the Presidential Management Council "Quick Silver" task force.
Electronic Credential Provider	An entity recognized by the Federal PKI Policy Authority or comparable entity as having the authority to verify the association of attributes or token to an identity.
End Entity	End-users.
Federal Bridge Certification Authority (FBCA)	The Federal Bridge Certification Authority consists of a collection of Public Key Infrastructure components (Certificate Authorities, Directories, Certificate Policies and Certificate Practice Statements) that are used to provide peer to peer interoperability among Entity Principal Certification Authorities.
Federal Public Key Infrastructure Policy Authority (FPKI PA)	The Federal PKI Policy Authority is a federal government body responsible for setting, implementing, and administering policy decisions regarding PKI interoperability that uses the FBCA.
Firewall	Gateway that limits access between networks in accordance with local security policy.
Integrity	Protection against unauthorized modification or destruction of information. A state in which information has remained unaltered from the point it was produced by a source, during transmission, storage, and eventual receipt by the destination.
Key Pair	Two mathematically related keys having the properties that (1) one key can be used to encrypt a message that can only be decrypted using the other key, and (ii) even knowing one key, it is computationally infeasible to discover the other key.
Level of Assurance	How much confidence there must be that the transaction participant is really who they claim to be.
Memorandum of Agreement (MOA)	Agreement between the Federal PKI Policy Authority and an Entity allowing interoperability between the Entity Principal CA and the FBCA.
Mutual Authentication	Occurs when parties at both ends of a communication activity authenticate each other (see authentication).

Term	Definition
Non-Persistent Cookie	A web browser cookie that is stored temporarily in RAM while the computer is running and the web browser is in use. It is removed at the time the browser is closed or the computer is turned off.
Non-Repudiation	Assurance that the sender is provided with proof of delivery and that the recipient is provided with proof of the sender's identity so that neither can later deny having processed the data. Technical non-repudiation refers to the assurance a Relying Party has that if a public key is used to validate a digital signature, that signature had to have been made by the corresponding private signature key. Legal non-repudiation refers to how well possession or control of the private signature key can be established.
Persistent Cookie	A web browser cookie that stored on the user's computer hard drive and not removed when the browser is closed or the computer is turned off.
Physically Isolated Network	A network that is not connected to entities or systems outside a physically controlled space.
Policy Management Authority (PMA)	Body established to oversee the creation and update of Certificate Policies, review Certification Practice Statements, review the results of CA audits for policy compliance, evaluate non-domain policies for acceptance within the domain, and generally oversee and manage the PKI certificate policies. For the FBCA, the PMA is the Federal PKI Policy Authority.
Principal CA	The Principal CA is a CA designated by an Entity to interoperate with the FBCA. An Entity may designate multiple Principal CAs to interoperate with the FBCA.
Privacy	Restricting access to subscriber or Relying Party information in accordance with applicable law and policy.
Private Key	(1) The key of a signature key pair used to create a digital signature. (2) The key of an encryption key pair that is used to decrypt confidential information. In both cases, this key must be kept secret.
Proxy login	User login provided by one application on behalf of other applications..

Term	Definition
Pseudonymous Access	Authenticated unidentified access, where authentication of identity is assured by trusted third-party and actual identity of subscriber is unknown directly by the agency application..
Public Key	(1) The key of a signature key pair used to validate a digital signature. (2) The key of an encryption key pair that is used to encrypt confidential information. In both cases, this key is made publicly available normally in the form of a digital certificate.
Public Key Infrastructure (PKI)	A set of policies, processes, server platforms, software and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key certificates.
Relying Party	Entity that relies upon the subscriber's credentials, typically to process a transaction or grant access to information or a system.
Repository	A database containing information and data relating to electronic credentials; may also be referred to as a directory.
Responsible Individual	A trustworthy person designated by a sponsoring organization to authenticate individual applicants seeking certificates on the basis of their affiliation with the sponsor.
Risk	An expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result.
Risk Tolerance	The level of risk an entity is willing to assume in order to achieve a potential desired result.
Server	A system entity that provides a service in response to requests from clients.
Signature Certificate	A public key certificate that contains a public key intended for verifying digital signatures rather than encrypting data or performing any other cryptographic functions.
Subscriber	A Subscriber is an entity that (1) is the subject named or identified in a electronic token issued to that entity, (2) holds or knows (typically a key or password) that can be used to authenticate the subscriber remotely.

Term	Definition
Technical non-repudiation	The contribution public key mechanisms to the provision of technical evidence supporting a non-repudiation security service.
Threat	Any circumstance or event with the potential to cause harm to an information system in the form of destruction, disclosure, adverse modification of data, and/or denial of service.
Token	Hardware or software that contains or can be used to generate cryptographic keys. Examples of hardware tokens include smart cards and memory cards. Software tokens include both software cryptographic modules that store or generate keys and storage devices or messages that contain keys (e.g., PKCS #12 messages).
Trust List	Collection of trusted certificates used by Relying Parties to authenticate other certificates.
Trusted Agent	Entity authorized to act as a representative of an Entity in confirming Subscriber identification during the registration process. Trusted Agents do not have automated interfaces with Certification Authorities.
Trusted Certificate	A certificate that is trusted by the Relying Party on the basis of secure and authenticated delivery. The public keys included in trusted certificates are used to start certification paths. Also known as a "trust anchor".
Trusted Timestamp	A digitally signed assertion by a trusted authority that a specific digital object existed at a particular time.
Trustworthy System	Computer hardware, software and procedures that: (1) are reasonably secure from intrusion and misuse; (2) provide a reasonable level of availability, reliability, and correct operation; (3) are reasonably suited to performing their intended functions; and (4) adhere to generally accepted security procedures.
Validate/validation	Establishing the status of an electronic credential presented by the subscriber through an authentication protocol.